Was ist Bitcoin?

Fallen, Gefahren und Tipps

- Software-Entwickler
- > 10 Jahre Berufserfahrung
  - Verteilte Systeme u. Web-Anwendungen
  - Von Startup bis Software für Versicherungen
- Journalistische Tätigkeit
  - https://blockchain-investment.at
  - https://www.kryptologen.de
  - https://coinkurier.de

Ing. Martin Keiblinger, Bsc.

1. Problem identifizieren
2. Lösungsmöglichkeiten überlegen
3. Werkzeuge kaufen oder bauen
4. Problem lösen

Lösung für welches Problem?


HOLDER LETTER
June 19, 2014

Ideologischer Hintergrund

- "Ein Geist geht um, der Geist der Kryptoanarchie"
- Kein Zugriff durch Dritte
  - ~~Staat~~
  - ~~Große Unternehmen~~
  - ~~Nachbar~~
- Verwandte Themen
  - Kryptoanarchismus
  - Darknet (The Onion Routing Network)

Ideologischer Hintergrund

- Geldschöpfung in privater Hand
- Österreichische Schule
  - Friedrich August v. Hayek
  - Ludwig von Mises
  - Etc.
- Konkurrenz von Währungen

Jahr	Medianeinkommen (€)	Lohnsteigerung (%)	Inflation (%)	Kaufkraft
1998	14,686.00	0.73	0.80	99.92
1999	14,929.00	1.63	2.00	99.52
2000	15,399.00	3.05	2.30	100.20
2001	15,530.00	0.84	1.70	99.32
2002	15,706.00	1.12	1.30	99.13
2003	15,863.00	0.99	2.00	98.11
2004	16,131.00	1.66	2.10	97.65
2005	16,631.00	3.01	1.70	98.87
2006	16,918.00	1.70	2.20	98.34
2007	17,376.00	2.64	3.20	97.70
2008	17,756.00	2.14	0.40	99.39
2009	18,333.00	3.15	1.70	100.78
2010	18,366.00	0.18	3.60	97.32
2011	18,529.00	0.88	2.60	95.63
2012	18,842.00	1.66	2.10	95.17
2013	19,057.00	1.13	1.50	94.80
2014	19,344.00	1.48	0.80	95.44
2015	19,558.00	1.09	0.90	95.62
2016	20,543.00	4.79	2.10	98.10

Das Problem

- Geldschöpfung in staatlicher Hand
- Geldfluss kann
  - Überwacht werden
  - Gestoppt werden

Ziel:

- Anonymität
- Autonomie

Was ist Bitcoin?

Währung

- Tauschmittel
- Eigenschaften
  - Transportierbar
  - Teilbar
  - Haltbar
  - Kaufkräftig
  - Einheitlich

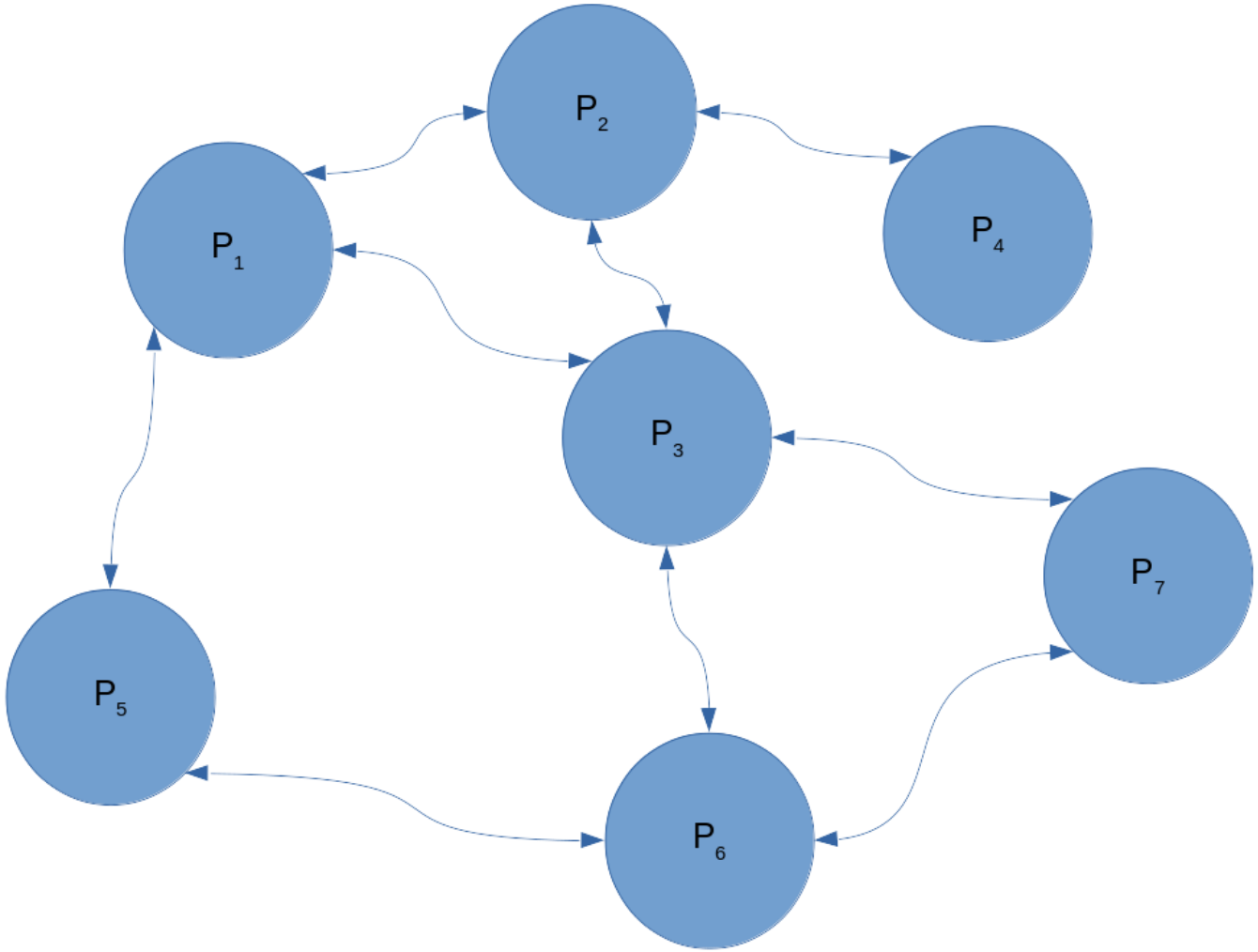
Transaktionssystem

- Kassabuch
- Aufzeichnung von Vermögensübertragungen
- Überprüfung und Validierung von Transaktionen
- Unterbrechungsfreier Transfer von Besitz
- Automatisierte Geldschöpfung
  - Endliche Anzahl von Bitcoin
  - Algorithmus zur "Erzeugung"

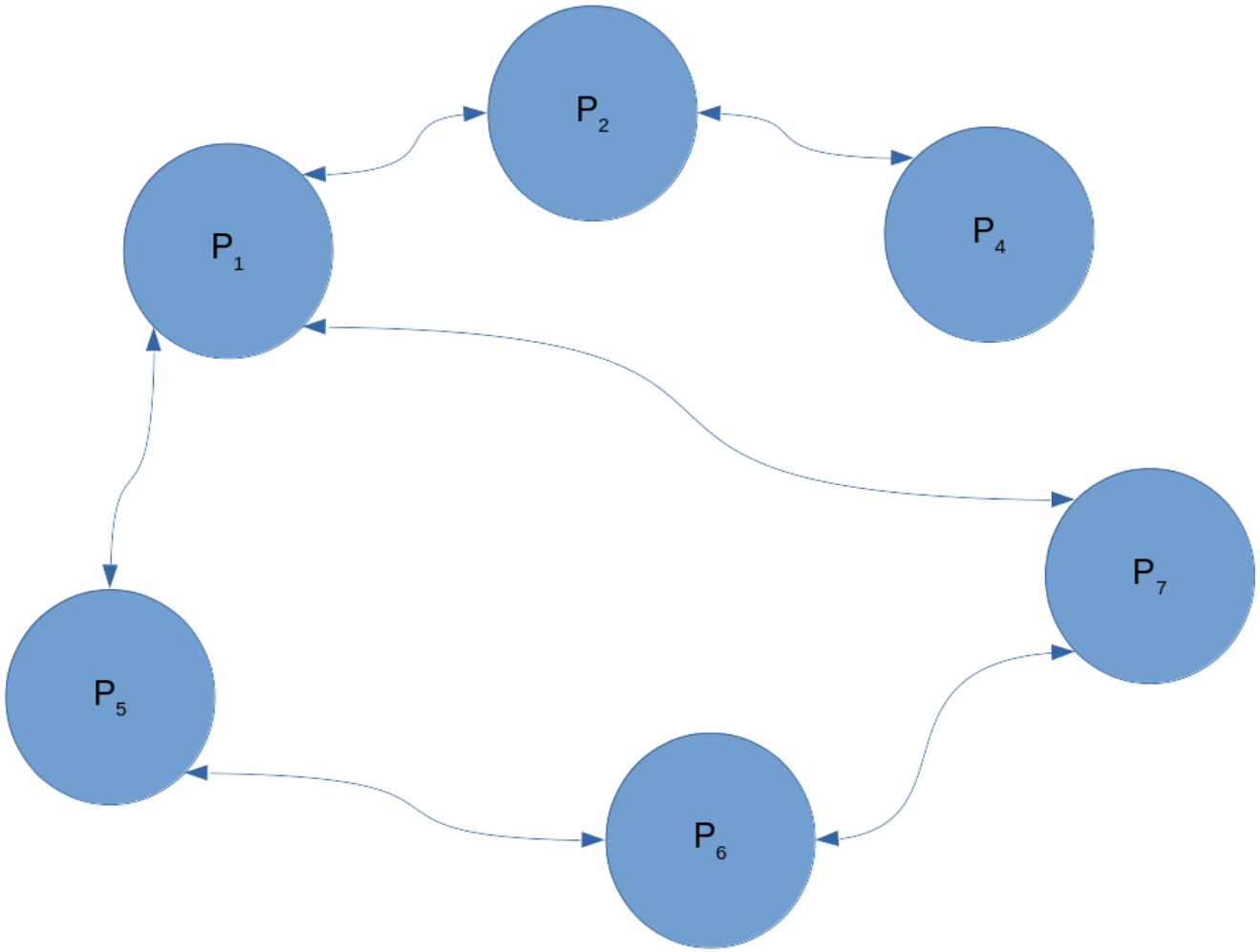
Wie macht das Bitcoin?

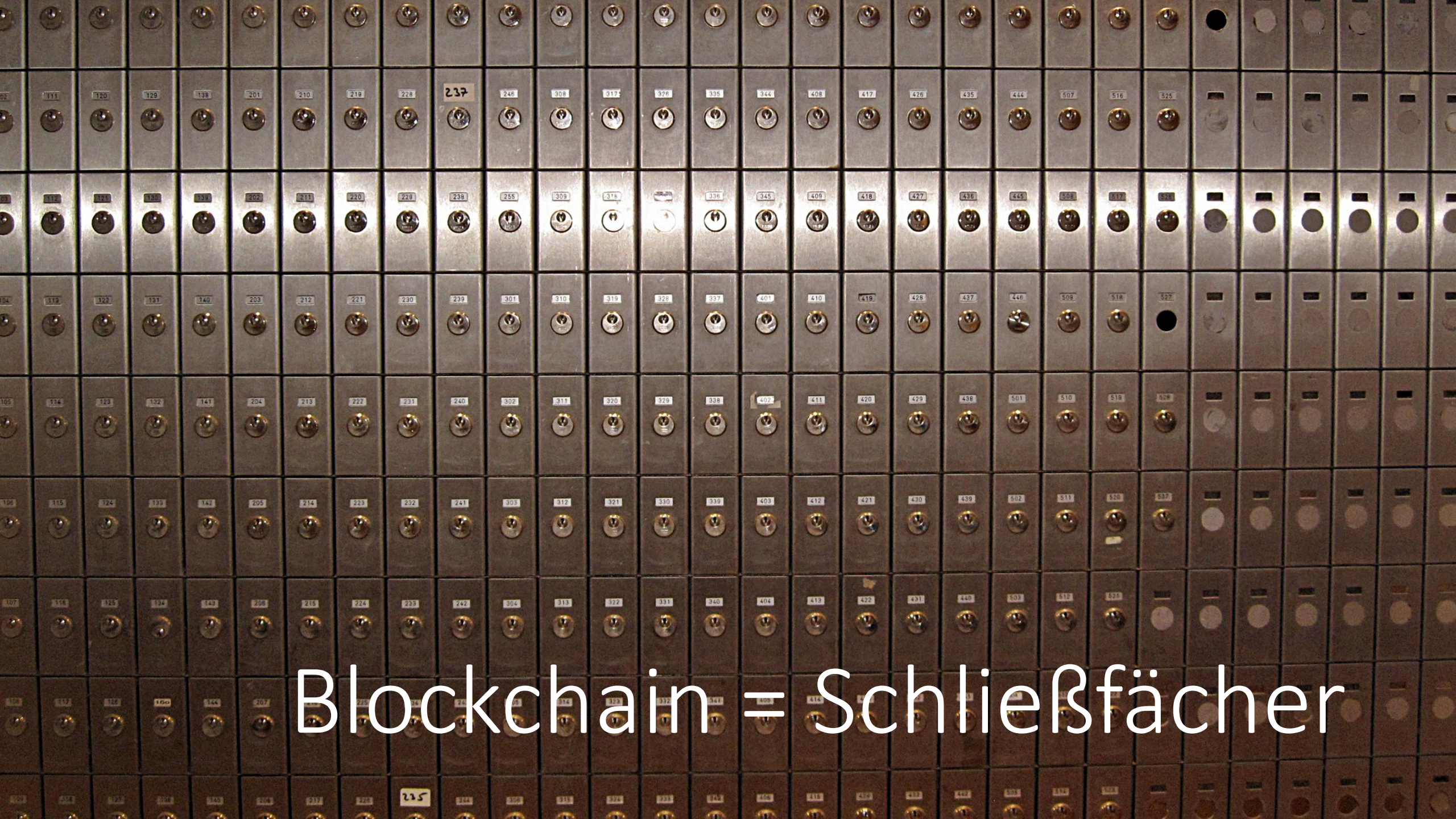
- Peer to Peer Netzwerk
  - Ausfallsicher
  - Dezentral --> Keine Zentralgewalt
- Kryptographie
  - Absicherung ohne zentralen Vermittler
  - Pseudonymität
- Dezentraler Konsensmechanismus
  - Blockchain
  - Mining

Peer to Peer Netzwerk



Peer to Peer Netzwerk




Blockchain = Schließfächer

Blockchain

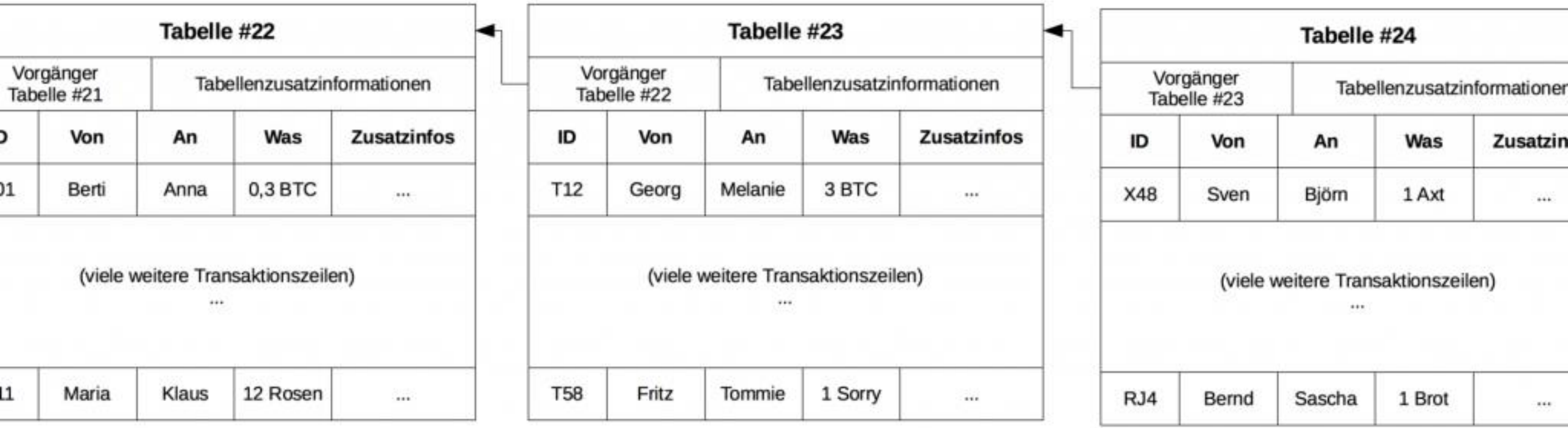
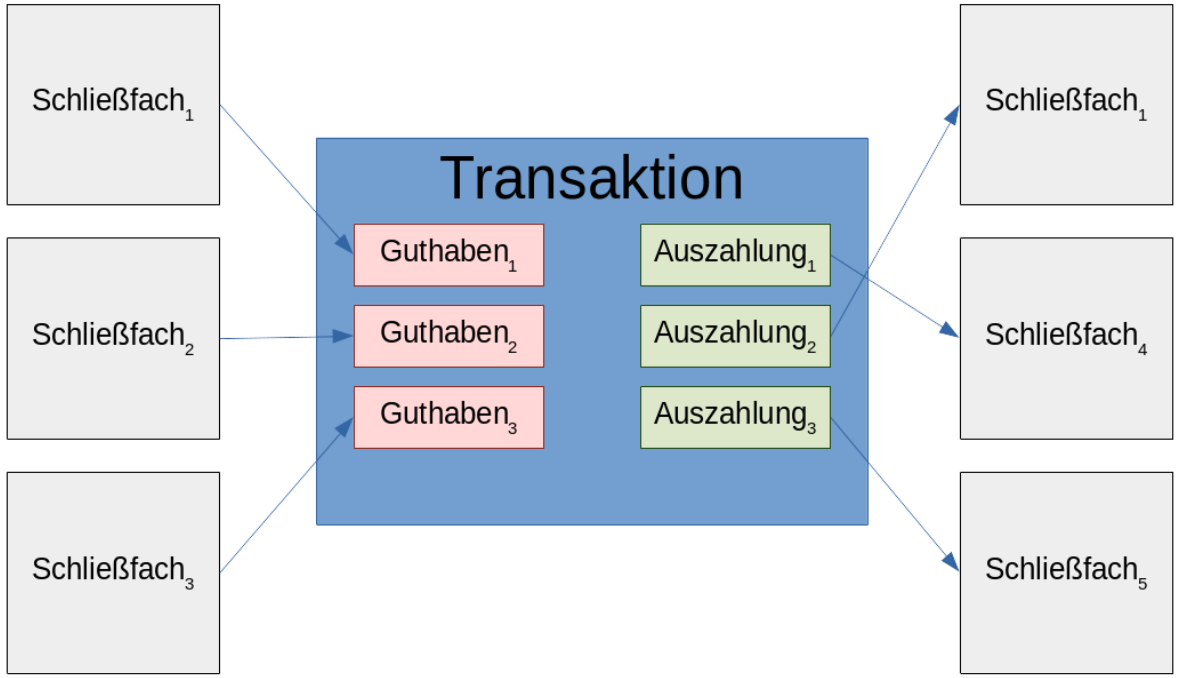


Tabelle #22
Vorgänger Tabelle #21
Tabellenzusatzinformationen
D
Von
An
Was
Zusatzinfos
01
Berti
Anna
0,3 BTC
...
(viele weitere Transaktionszeilen)
...
11
Maria
Klaus
12 Rosen
...
Tabelle #23
Vorgänger Tabelle #22
Tabellenzusatzinformationen
ID
Von
An
Was
Zusatzinfos
T12
Georg
Melanie
3 BTC
...
(viele weitere Transaktionszeilen)
...
T58
Fritz
Tommie
1 Sorry
...
Tabelle #24
Vorgänger Tabelle #23
Tabellenzusatzinformationen
ID
Von
An
Was
Zusatzin
X48
Sven
Björn
1 Axt
...
(viele weitere Transaktionszeilen)
...
RJ4
Bernd
Sascha
1 Brot
...


Transaktion

Transaktionen

- Schließfächer mit Einwegschlössern
- Jede Verwendung -> neues Schloss



Blockchain

- Block
  - Liste von bestätigten Transaktionen
  - Kryptographische Absicherung
  - Zeiger auf vorherige Transaktion
- Blocklänge ("Blockhöhe")
  - Konsensmechanismus
  - Abgleich in dezentralem Netzwerk
- Mining
  - "Erlaubnisbestätigung" des Blockerzeugers

Geldschöpfung (Mining)

Rollen im Bitcoin-Netzwerk

- "Full Node" - Vollwertiger Netzwerkknoten
  - Speichert komplette Bitcoin-Blockchain
  - Alle jemals getätigten Transaktionen
  - Viele Gigabyte Speicherverbrauch
  - Transaktionen "empfangen" und senden
- "Light Node"
  - Transaktionen "empfangen" und senden
  - Abhängig von Full Node
- Schürfer (Mining) -> Bestätigen von Transaktionen
  - Rätsel lösen
  - Transaktionen und Zufallszahl -> "Errechnen" von Erlaubnis

Konsensmechanismus

- Block-Erzeugung
  - Ca. Alle 10min neuer Block
  - Ca. 3.500 Transaktionen pro Block
  - Ca. 6 Transaktionen pro Sekunde
- Alle Peers überprüfen Block
  - Kryptographische Absicherung für Gültigkeit
- Konsensmechanismus
  - Block mit längster Kette -> Gültiger Block
  - Überprüfung von Block günstig/schnell
  - Erzeugen von Block teuer/langsam

Bitcoin-Wallet

- Bitcoin-Geldbörse / Wallet
  - Schlüsselkette
  - Viele Schlüsseln - viele Schließfächer
  - Zusätzliche Schutzmaßnahmen
  - Beliebig viele und gratis
- Personal Computer
  - Speichert "Schlüsselkette"
  - Speichert Kopie der Blockchain (vielleicht)
- Bitcoin-Netzwerk -> viele andere Computer


NYSE
The world puts its stock in us

Bitcoin Ökosystem

- "Scam" - Viel Betrug und falsche Versprächungen
  - MLM- und Pyramidensystembetrügerein
  - Arbitrage-Bots
  - Copy-Trading und Signal-Gruppen
  - Malware- und Bitcoin-Fork-Scams
- Exchanges
  - Börsen um Online Kryptowährungen zu kaufen
  - Prüfen ob vertrauenswürdig!
  - Österreichische Firma: Bitpanda

Exchanges (Börsen)

- Überprüfen Identität
  - "Know your Customer" KYC
- Online-Wallets in Börsen
  - Erlauben bequemen u. schnellen Handel
  - "Not your keys? Not your bitcoins!"
- Auskunft an Finanzamt
  - Haltefristen
  - Steuersätze
  - Führen Sie Aufzeichnungen!

Datensicherheit

- Verlieren Sie nicht 7.500 BTC auf der Mülldeponie!
- Computersicherheit
  - Updates installieren
  - Anti-Viren-Software aktuell halten
- Teilen Sie Ihr Vermögen auf verschiedene Wallets auf
  - Verschiedene Schlüssel!
- Backup, Backup, Backup!
  - Paper-Wallet
  - Steel-Wallet
  - Daten auf mehrere Orte verteilten
- Adressen nur einmal verwenden

Cold-Storage

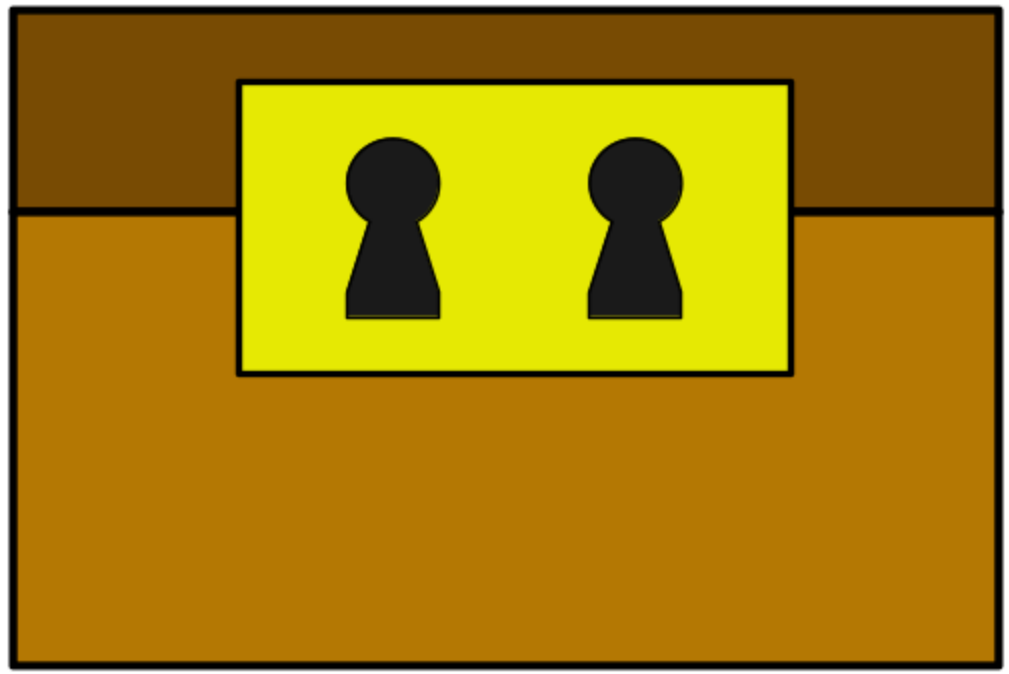
- "Kalte" Geldbörsen
  - Nicht für Transaktionen zu verwenden
- Können "heiß" gemacht werden
  - Wallet kann auf Computer aktiviert werden
- Kein Virus der Welt kann ein Blatt Papier im Schrank lesen!

Hardware-Wallet

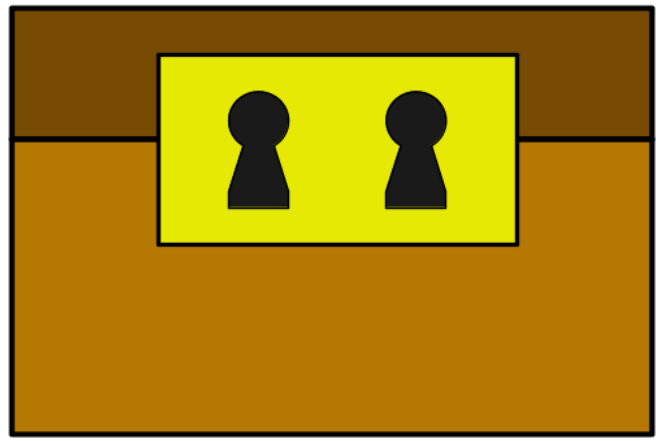
- 2FA – Zwei Faktoren für die Authorisierung
  - Passworteingabe
  - Hardware in Form USB-Stick (mit Knopf)
- Zusätzliche Hürde, zusätzliche Sicherung
- Verschiedene Hersteller
  - Backup trotzdem nötig!
  - Hardware auch aktualisieren!

Kryptographie

- Public Key Kryptographie
  - Verschlüsselung
  - Signierverfahren
- Hash-Verfahren

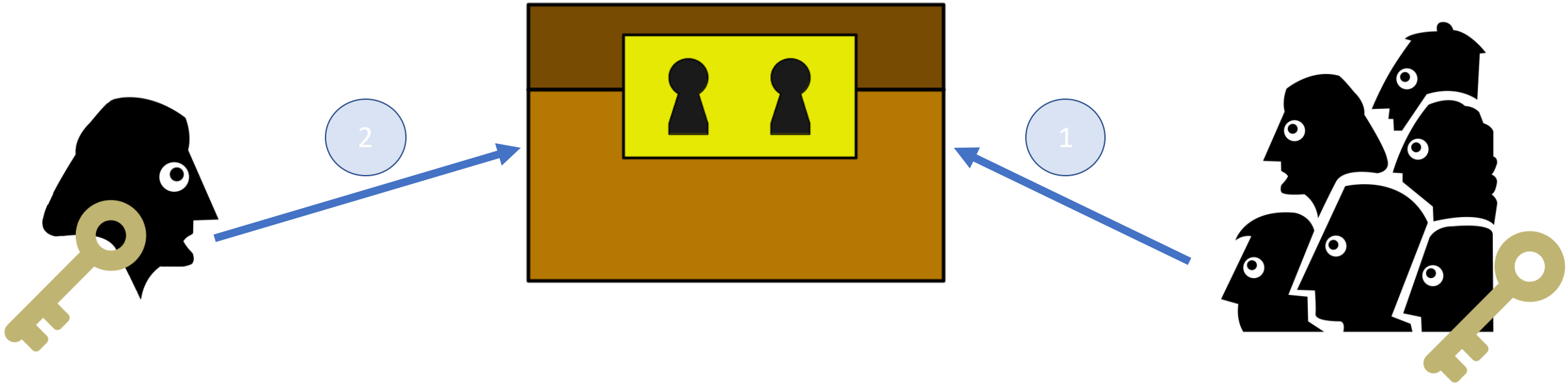


Privater Schlüssel



Öffentlicher Schlüssel

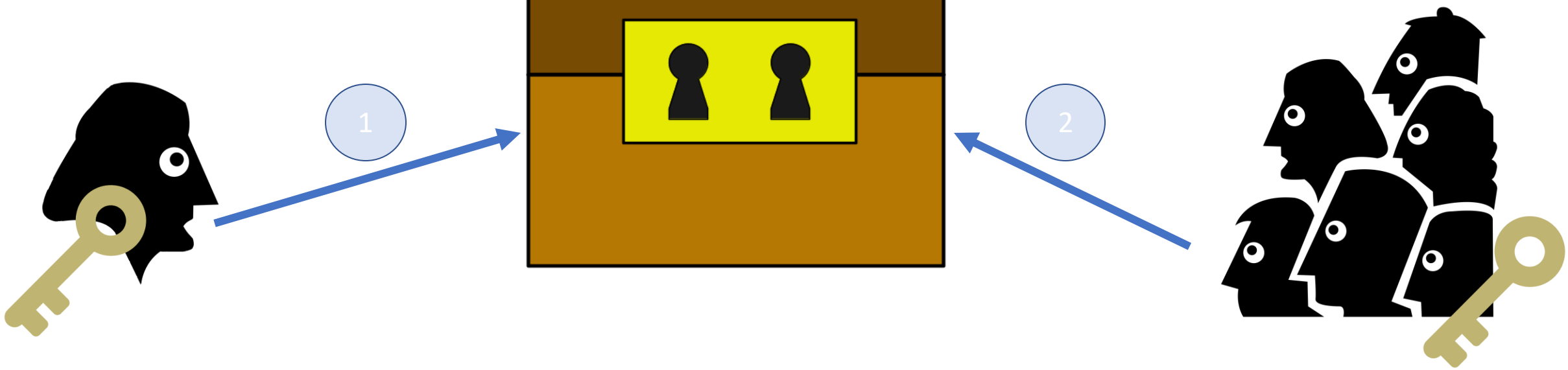
Verschlüsselung



Privater Schlüssel
für das Entsperren

Öffentlicher Schlüssel
für das Zusperren

Signieren



Privater Schlüssel
für das Zusperren

Öffentlicher Schlüssel
für das Aufsperren

Hash-verfahren

- Erzeugt Ergebnis für eine Eingabe
  - Nicht umkehrbar
  - Jede Eingabe, hat unterschiedliches Ergebnis (kollisionsfrei)
- Bitcoin SHA256
  - Mining
  - Validierung v. Transaktionen
  - Authorisierung -> Key Hash

Fragen?

Literaturverweise

- https://www.activism.net/cypherpunk/crypto-anarchy.html
- https://scholarium.at/
- https://www.ecb.europa.eu/ecb/tasks/html/index.en.html
- https://www.ecb.europa.eu/mopo/strategy/pricestab/html/index.en.html
- https://www.oenb.at/Geldpolitik/Umsetzung-der-Geldpolitik/Zinspolitik/Mindestreserve.html
- https://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/soziales/personen-einkommen/jaehrliche_personen_einkommen/index.html
- https://www.statistik.at/web_de/statistiken/wirtschaft/preise/verbraucherpreisindex_vpi_hvpi/index.html

Literaturverweise

- https://mises.org/library/denationalisation-money-argument-refined
- https://www.blockchain-investment.at/was-ist-eine-blockchain/
- https://www.blockchain-investment.at/uebersicht-ueber-krypto-investing/
- https://www.goodreads.com/book/show/36448501-the-bitcoin-standard
- https://github.com/bitcoinbook/bitcoinbook

Bildquellen

- Marathonlauf, https://www.flickr.com/photos/michalo/283653500
- Schließfächer, https://commons.wikimedia.org/wiki/File:Bad_Rothenfelde,_Sch%C3%BCchtermannklinik,_Reha-Abteilung,_Patientenschlie%C3%9Ff%C3%A4cher_f%C3%BCr_Mitteilungen.JPG
- Julian Assange, https://www.flickr.com/photos/dgcomsoc/14933990406
- Börse, https://www.pexels.com/de-de/foto/aktien-borse-borsenparkett-business-259208/